In the initial stages of your digital development program — particularly if it was a pilot with a limited budget — your focus may have been on conducting research and development, building your program’s operations and tracking your results, rather than on limiting your legal liability or complying with national laws and regulations. If you’re now planning to scale your digital development solution, take it to a new geography, enter into new commercial partnerships or transition it to government, it’s a good time to take stock of your legal situation.

Preparing your program for the next phase means reviewing and revising your service and partner contracts and developing proactive policies in areas such as user privacy, user consent and intellectual property (IP). As with the other program elements that you are revisiting, a thorough reassessment of the landscape in which your solution operates is required. Laws and regulation are constantly evolving in areas such as data protection.

In earlier stages, in-house knowledge of legal implications may have sufficed, but at this stage of scale, professional legal advice is warranted. Expert consultation from a law firm with telecommunications and ICT expertise can help you evaluate your existing contracts and compliance with relevant regulations. While legal consultation can be expensive, building legal costs into your budget can help avoid costly fines or liabilities in the future.
This module draws on interviews conducted with digital development leaders in organizations including BBC Media Action, Esoko, Kapil Sapra & Associates, TaroWorks, Kopo Kopo, Cell-Life, Signum Advocates and Vital Wave. The examples they share highlight the challenges and pitfalls they navigated on the road to scale and sustainability. Note that the nature and sequence of the steps contained in this module are highly dependent on the vertical, sector and geography in which your solution operates, and many of the steps may happen in parallel.

After reading this module, you’ll be able to plan your next legal steps, including how to:

1. Assess the impact of evolving laws, policies and regulations on compliance
2. Ensure a flexible contracting approach to accommodate changes
3. Clarify ownership of intellectual property
4. Review software, hardware and content licensing terms
5. Clarify, limit and manage liability
6. Review and update service level agreements

Disclaimer: All templates and guidance provided in this guide are illustrative only and should not be considered legal advice. Readers should seek professional legal advice prior to executing any contracts or agreements.
Key steps

1. **ASSESS THE IMPACT OF EVOLVING LAWS, POLICIES AND REGULATIONS ON COMPLIANCE**
   - Assess legal, regulatory and policy changes in your digital landscape
   - Monitor evolving laws on data privacy and protection
   - Get informed user consent that enables expansion or transition
   - Comply with data-hosting laws and regulations

2. **ENSURE A FLEXIBLE CONTRACTING APPROACH TO ACCOMMODATE CHANGES**
   - Create or renegotiate master agreements with key partners
   - Use addenda to make changes to scope of work, commercial terms and timeframes
   - Create mechanisms for managing changes to your solution

3. **CLARIFY OWNERSHIP OF INTELLECTUAL PROPERTY (IP)**
   - Make sure your employee contracts prevent IP confusion or disputes in the future
   - Clarify IP ownership in contracts with technical partners or vendors
   - Ensure that you have the right to use solution content

4. **REVIEW SOFTWARE, HARDWARE AND CONTENT LICENSING TERMS**
   - Ensure hardware and software licenses allow for transition of program ownership
   - Negotiate reduced software license costs for increased scale
   - Assess restrictions for open source or Creative Commons licenses

5. **CLARIFY, LIMIT AND MANAGE LIABILITY**
   - Determine who assumes liability and under what circumstances
   - Cap liability at a manageable level
   - Ensure effective indemnification
   - Consider the liability of open source vs. proprietary software and content

6. **REVIEW AND UPDATE SERVICE LEVEL AGREEMENTS (SLAS)**
   - Define technical support requirements for scale
   - Ensure your technical partners can meet SLA requirements
   - Watch out for penalty clauses
Assess legal, regulatory and policy changes in your digital landscape

In the first few years of your program’s operations when the number of users was relatively small, you may not have needed to focus heavily on legal, regulatory and policy considerations. Yet to operate at scale, your digital development solution will not only need to comply with laws, regulations and policies designed to protect end users and their personal data, it will also have to align and comply with policy and regulatory frameworks at the national or sub-national level in different sectors, which have likely evolved since your operations began.

For example, many countries have adopted national strategies in digital health, financial services and education to ensure that solutions align with their policy and program priorities and to promote solution interoperability and scalability. In addition, in highly regulated industries such as financial services and health, government ministries and agencies constantly issue updates to regulation and policy guidance that affect compliance with operators of any solution, digital or otherwise — such as Know Your Customer (KYC) and settlement requirements for payments solutions. It’s important to review strategy documents, legislation and policy guidance relevant to your solution, but it’s also worth regularly talking to your contacts in government about what their requirements mean for your solution’s ability to comply. They may also be able to advise you on how you can get involved in the committees and advisory groups that shape these policies.

Monitor evolving laws on data privacy and protection

Laws and regulations designed to protect and limit the use of people’s personal information vary widely from country to country. They are also constantly evolving and subject to change by lawmakers and regulators. It’s important to stay up to date with these laws because they may have significant implications for the design and delivery of your digital solution. As countries with little or no regulation implement laws, you’ll need to monitor them closely with your legal adviser and ICT partners, including mobile network...
**In practice | BBC Media Action**

**The challenges of taking informed consent from low-income, low-literate users**

One of the reasons we set up a call center in Bihar, India was to try to keep our database of more than 100,000 Community Health Workers (CHWs) up-to-date and accurate. Ninety-eight percent of CHWs in the state are pay as you go mobile customers, and change their SIM cards regularly in response to MNOs’ special offers.

As a result, CHWs’ mobile numbers are frequently changing, which makes it challenging to monitor and report on their take up and usage of our reproductive, maternal, neonatal and child health (RMCH) education services (Mobile Kunji, an IVR and print-based Job Aid, and Mobile Academy, an IVR-based training course).

Before our call center could begin capturing personal data from CHWs, such as their name, mobile number and location, they needed to take their consent to comply with data protection legislation in India. Our legal advisers drafted a consent script designed to be read by call center agents to CHWs. Since the requirement of law is to take informed consent by letting the data providers (in this case, CHWs) know the purpose of collection; the details of the collector of the data, as well as processors and recipients of the data, the script had to be drafted carefully.

Further, the consent was not just required for use by BBC Media Action, but also by its partners to meet the objective of the project. The script was accordingly drafted, stating that the data was being captured on behalf of the government, and would be stored, processed and used by BBC Media Action and its partners to deliver specific mHealth education services, up until a specific date, as part of a specific program.

After the script was drafted and translated into Hindi, we then user-tested it with CHWs. Unsurprisingly, we found that typical consent terms such as ‘data’, ‘database’, and even ‘service’ and ‘processing’ (in the context of mobile services) were alien to most rural women in Bihar and hence it was not possible to take typical ‘informed consent’. Thus, the language in the consent script had to be modified to make it comprehensible to low income, low illiterate rural women, so that they could give genuinely ‘informed’ consent.

Our legal advisors also advised us on the mode of obtaining consent, and storing such consent, to be able to prove consent, if the need arose. To meet the requirements of different laws, each call had to be recorded and the consent stored in the form of an audio file for a period of three years after the completion of purpose for which the data was collected.
operators (MNOs), technology solution providers and data-hosting companies. Regulatory requirements, standards and laws that you’ll need to monitor include those that govern data privacy, payment and settlement systems (if digital payments are involved), digital marketing (such as telemarketing calls), use and transmission of personal data (such as medical records) and user consent (see below). Most national governments require that such laws and regulations be published on government websites with a point of contact in both national and sub-national governments.

Get informed user consent that enables expansion or transition

While laws vary widely between countries, you normally need to get each user’s consent to capture, store and use their personal information. Most consent laws stipulate that you must explain to the user why you want to capture their data and how you’re going to use it in order for them to give you informed consent. What varies is who is responsible for obtaining consent from users and how consent is obtained, recorded and stored. Consent is especially important when collecting data for research purposes.

If you’re considering scaling your solution to new geographies, working with new partners or transitioning to government, you’ll need to make sure that you already have consent from your users to give partners access to their data or that their existing consent permits relevant changes to how their data will be handled. Otherwise you’ll need to obtain new consent. Without that specific informed consent, it might not be legal to allow a third party to access their information. In some countries, compliance depends on how laws and regulations assign responsibility to those collecting the data compared to those who process or store the data. It’s worth consulting with a lawyer and an ethics review board to ensure that the consent language that needs to be communicated to your users is short, accurate and easy to comprehend yet broad enough to enable expansion and transition in the future.

Comply with data-hosting laws and regulations

Each country has different laws about where users’ data can be hosted. For example, countries such as China, India, Indonesia and Nigeria do not allow any identifiable user data to be sent or stored outside the country. Other countries, for example, South Africa, don’t explicitly prohibit transmission of data across borders but may insist on such a ban for digital solutions in areas such as public health or education. The sensitivity of the data may influence where and how it can be hosted or transferred, and countries define sensitive in diverse ways. Cloud-based hosting may be cheaper and easier to maintain, but if the servers where data resides are in another country and transmitting data to them violates government regulations, you’ll have to find another way forward. Complying with these laws and regulations could have serious implications for your software and hardware decisions, technical support solutions and costs at scale. In addition to talking with your lawyers about this issue, have conversations with your vendors and solution partners about options and relevant regulations, especially those who work in multiple geographies and navigate these issues regularly.
Other examples

Watch Kenneth Muhangi, Managing Partner at Signum Advocates, talk about compliance with data privacy laws in Uganda.

Watch Brent Chism, CEO of TaroWorks talk about ensuring compliance with local markets for a merchant payment solution in Tanzania.

In order to ensure the personal data collected from expectant mothers and stored by the MomConnect program of South Africa's National Department of Health would be protected, partners worked with the government to develop a data transfer and privacy protocol. This is a standardized format and process for transmitting data safely between devices, which allowed them to safely host the data on a server within South Africa. Read more about MomConnect here.

How to

Compare the strength of international data-hosting and transfer laws here and learn more about international data security standards here.

See detailed examples of data protection legislation in South Africa here.

View the Mobile Privacy Principles, based on recognized and internationally accepted principles on privacy and data protection here.

See an example of informed consent language for mobile health solutions here and a compilation of national standards for privacy and data protection in over 100 countries here.
ENSURE A FLEXIBLE CONTRACTING APPROACH TO ACCOMMODATE CHANGE

Create or renegotiate master agreements with key partners

You can save yourself considerable time and legal fees if you create a flexible legal framework for each key partnership in the form of a master agreement. This agreement defines and covers the legal terms of the relationship between contracting parties, addressing topics such as intellectual property (IP), liability, indemnity, renewal, termination and data protection, which may remain relatively static for an extended period.

Specifics about geography, scope of work, project plan and commercial terms, which are likely to change as your program grows, can then be attached to the master agreement as annexes. These might take the form of separate annexes covering discrete topics or a single statement of work.

Use addenda to make changes to scope of work, commercial terms and timeframes

If you have a master agreement in place and your program and agreements with partners and vendors need to change, then changes in the scope of work, project plan, geography, timeframe or commercial terms can be executed as addenda and attached as separate annexes to the master agreement. The content of these addenda can be specified by technical or commercial in-house staff working on the project in collaboration with their technical or commercial partners. However, for such addenda to have legal and binding effect, they must be executed according to the procedure specified in the master agreement and by the people authorized to do so.

This approach allows your legal counsel more flexibility, because they won’t have to renegotiate the legal terms in the master agreement every time your program changes. This step can reduce legal review from several hours to as little as 15 minutes. Your legal adviser could even produce a standard template for addenda which will make it even quicker and easier to update specific terms.
In practice | Kapil Sapra & Associates

Watch Kapil Sapra from Kapil Sapra & Associates explain how to structure legal agreements to enable and accommodate scaling up or down, or transition of ownership to a partner.

Other examples

- Watch Kenneth Muhangi, Managing Partner at Signum Advocates, talk about why you need to have an ICT lawyer.

- Watch Brent Chism, CEO of TaroWorks, talk about his time at Kopo Kopo and why they needed a lawyer when expanding to new markets.

How to

- See a sample master services contract for IT services here
- Read about the steps involved in designing an effective change control process here
Create mechanisms for managing changes to your solution

When planning the expansion of your digital program, having clear change control mechanisms can help you execute and track amendments to your partners' scope of work. Change control is the process through which requests to change a project or solution are evaluated and acted on. Changes can include enhancement to connectivity infrastructure or modifications to the content you provide to users of your solution. For such changes, formal contract addenda may not be required. As with contract addenda and SOWs, creating templates in advance for changes that you and your partners mutually agree to will minimize confusion or disruption, as will clear communication processes for making changes. However, you need to clearly identify the provisions that can be modified through change control mechanisms. Change control agreements should be easy to comply with for both your team and your partners' and as free from legal jargon as you can make them.
When planning the expansion of your digital program, having clear change control mechanisms can help you execute and track amendments to your partners’ scope of work.
## Protected Health Information (PHI) in the United States

Personal information in the U.S. is governed by broad national and state privacy laws, but in the health sector this data is governed by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA states that anyone who creates, receives, maintains or transmits PHI is legally responsible for protecting it from falling into the hands of anyone who does not legally have access to it. The law classifies the following data as PHI.

<table>
<thead>
<tr>
<th>1. Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. All geographical identifiers smaller than a state, except for the initial three digits of a postal address code</td>
</tr>
<tr>
<td>3. Dates (other than years) directly related to an individual</td>
</tr>
<tr>
<td>4. Phone numbers</td>
</tr>
<tr>
<td>5. Fax numbers</td>
</tr>
<tr>
<td>6. Email addresses</td>
</tr>
<tr>
<td>7. Social Security numbers</td>
</tr>
<tr>
<td>8. Medical record numbers</td>
</tr>
<tr>
<td>9. Health insurance beneficiary numbers</td>
</tr>
<tr>
<td>10. Account numbers</td>
</tr>
<tr>
<td>11. Certificate/license numbers</td>
</tr>
<tr>
<td>12. Vehicle identifiers and serial numbers, including license plate numbers</td>
</tr>
<tr>
<td>13. Device identifiers and serial numbers</td>
</tr>
<tr>
<td>14. Web Uniform Resource Locators (URLs)</td>
</tr>
<tr>
<td>15. Internet Protocol address numbers</td>
</tr>
<tr>
<td>16. Biometric identifiers, including finger, retinal and voice prints</td>
</tr>
<tr>
<td>17. Full face photographic images and any comparable images</td>
</tr>
<tr>
<td>18. Any other unique identifying number, characteristic or code except the unique code assigned by a specific service provider</td>
</tr>
</tbody>
</table>

### Minimum civil penalty for violation:
$100 per violation, with an annual maximum of $25,000 for repeat violations

### Maximum civil penalty for violation:
$50,000 per violation, with an annual maximum of $1.5 million

### Maximum criminal penalty for violation:
A fine of up to $250,000 or imprisonment up to 10 years

Source
Data protection requirements differ depending on where you are in the world. Failing to protect the personal data of your customers, users or beneficiaries can result in severe consequences. The examples shown here illustrate how different the rules can be from country to country, and how important it is to know and adhere to them carefully.

**Sensitive Personal Data or Information (SPDI) in India**
In India, personal information refers to any information that relates to an individual that can be used either directly or indirectly to identify him or her. In September 2017, the Supreme Court of India cited the risks posed by digital data collection in ruling that privacy is a constitutional right, opening the door to stricter enforcement of data protection and use laws and regulations.

**Sensitive Personal Data or Information (SPDI)** is a subset of personal information that includes the following data. Information about individuals that is available or accessible in the public domain (assuming it complies with national laws) is not classified as SPDI.

1. **Passwords**
2. **Financial information such as bank account, credit or debit card, or other payment instrument details**
3. **Physical, physiological and mental health condition**
4. **Sexual orientation**
5. **Medical records and history**
6. **Biometric information**
7. **Any detail relating to these items that a company or organization collects, stores or processes to provide a service**

**Maximum civil penalty for violation:**
A fine up to INR 5,00,000 INR ($7,820)

**Maximum criminal penalty for violation:**
Imprisonment for a term of up to three years
Make sure your employee contracts prevent IP confusion or disputes in the future

Nearly all digital development programs involve the creation of IP relating to the content, hardware, software or other technology used to deliver a solution, and clarifying IP ownership with respect to your employees is a requirement for scale. Typically, any IP produced by a person during the term of their employment belongs to the organization that employed them. Implementers who have dealt with this issue suggest making sure that your employee contracts clearly define what “working for the organization” means. For example, does it refer only to work done during office hours when they are using office equipment, or does it include any professional activity? Does it cover only the IP produced by an employee individually or IP created jointly with other employees?

Employee contracts should include clauses specifying expectations around assignment and assumption, confidentiality, conflicting employments or engagements, and protection of third-party information (including personal data of customers or users). But including these items in contracts isn’t always enough to prevent problems. You need to train current employees and potential new hires to make sure they understand what these terms mean and the employment conditions around them.

Clarify IP ownership in contracts with technical partners or vendors

Contracts should specify the IP rights to work created by consultants, contractors or vendors. The terms of each contract may differ. If you want your program to own the IP in your digital solution, use a contract that clearly defines work produced by contractors or vendors as work for hire or made for hire and explicitly assigns the IP ownership to your organization. Make sure you limit the contractor’s or vendor’s right to use the IP to work related to the contract only and for a set period of time. It’s particularly important to resolve IP issues up front when collectively creating open source software, because sole IP ownership by one of the partner organizations can reduce confusion and simplify
In practice | BBC Media Action

Why we retain IP ownership, and control of our content through licensing

*BBC Media Action always retains ownership of the Intellectual Property (IP) in its content. This isn’t because we want to make money from selling it. And it’s not because we want to limit the use of our content; BBC Media Action regularly licenses its content for free to others.*

Rather, it’s because we need to retain control over the content as it has liability attached to it, and appropriately license our content to others without exposing ourselves to undue liability. The global recognition of the BBC brand is a huge opportunity, but it can also make us a target for legal action and reputational damage.

We were willing to license our content to third party aggregators/ MNOs to deliver our mobile health education services in India, despite having to accept hundreds of thousands of dollars of liability, because we had created it, owned it, and could confidently vouch for its accuracy. The situation would have been much more complicated if we hadn’t owned the IP in the content, or had shared the IP with other organizations. Our licensing terms also enabled us to control how much MNOs charged for the content (a rate we knew poor families could afford), and to control the geographies in which it would be accessible.

Controlling the location of distribution can be important, particularly with health information, because government health regulations, prevalence of diseases and availability of medical supplies and services vary from geography to geography. We would not want our content to be distributed in geographies where the information was inaccurate or against government regulations.

Our content license also does not allow modification by others; again, because we need to limit liability and ensure quality. If we allowed others to edit our content after licensing it, they could introduce factual inaccuracies. As the known creators of the content, this could expose BBC Media Action to legal action and reputational damage if the inaccuracies caused harm or offense. None of these precautions limits our commitment to global access to our content, through licensing.

How to

- Search WIPO Lex, the world’s most comprehensive source of data for international treaties and national laws and regulations about IP, [here](#)
- See a work for hire template [here](#)
- View a template for assigning ownership of IP created by employees to the organization who employs them [here](#) and a template for selling IP to another organization [here](#)
the process for expanding its distribution. Discussing IP ownership issues proactively with partners as you’re negotiating or renegotiating contracts can prevent expensive and disruptive disputes later on, especially as new IP is created.

Ensure that you have the right to use solution content

The technology your solution relies on is important, but so is the content it contains. You can create your own content, buy it from someone else, use open source content, crowdsource it or provide a platform for user-generated content. Regardless of which model you choose, you need to make sure you have the rights to distribute or publish content, modify it, sell it or transition it to the government without violating someone else’s copyright or licensing terms. If you are co-developing content with other organizations, consider the IP ownership issues discussed in the previous paragraph. If you’re transitioning ownership of a digital program to government or another organization, it may be possible to assign IP rights to the new owner while still retaining a right to use the IP in the future. Be sure to include such provisions in your contracts and written agreements.
Discussing IP ownership issues proactively with partners as you’re negotiating or renegotiating contracts can prevent expensive and disruptive disputes later on, especially as new IP is created.
Ensure hardware and software licenses allow for transition of program ownership

If you plan to transition your program to a government, it is critical to verify that your software and hardware licenses can be scaled up and transferred to a third party. Many proprietary software licenses are restricted to a specific project and time period and cannot be transferred without a new agreement. However, it may be possible to negotiate irrevocable licenses that are transferrable to a specified third party at no additional cost and in perpetuity. The possibility of any future expansions and transitions should ideally be part of your master agreement, even if these provisions are non-binding. Language allowing the replacement of an old contract with a new one without requiring permission from the vendor or provider should also be included. The transfer of hardware and software to a third party could also carry a significant tax burden, which needs to be evaluated by a tax expert.

Negotiate reduced software license costs for increased scale

Many proprietary software licenses are restricted by capacity — number of users, volume of messages or minutes, number of machines — which could make it impossible for you to scale without purchasing new licenses and incurring additional costs. Estimate the capacity that you’ll need at various levels of scale and negotiate reduced licensing costs as the scale of use increases. While it would be ideal to negotiate unlimited licenses, this is usually only possible with software providers who have a strong need for your business or see other advantages in granting a limitless license. If you have multiple vendor options, see if you can use that to your advantage in negotiating these terms.

Assess restrictions for open source or creative commons licenses

Open source software and content is also covered by licenses, which can be quite restrictive. For example, these licenses may require use of the content or software purely for not-for-profit use. Or they may state that the content or software can only be offered to
In practice | Esoko

Licensing our platform and content to resellers

In order to scale our agricultural market pricing platform into new countries we adopted a reseller model where we licensed use of our platform and our content to external organizations. Our agreements with resellers clearly state that when licensing our platform we still retain full IP rights for both the software platform and the content created for it. This remains true even if we develop specific features or content for a reseller.

In some cases, we build in clauses to our agreements that restrict us from sharing content that we have developed for a single reseller with any others. This provides the reseller with exclusive use of specific, licensed content even if we retain the IP. We also restrict our resellers from sharing any content they have licensed from us without our written consent.

How to

▶ See a template for a content licensing agreement here
▶ Read a list of FAQs related to Creative Commons licenses in a global health context here
▶ Read about software ownership and long-term sustainability issues in digital development programs here

low-income end users, in cases where the license owner is making money from sales to middle-income audiences and doesn’t want to undermine their core business. The terms of the license may also not allow you to take the content or software to a new country or sub-license it to a third party, such as the government.

Many content licenses, including certain Creative Commons licenses, do not allow modification of the content because of liability concerns. In other words, if you modify the content and introduce errors or biases into it, then the creator and licensor of the content may still be found liable by a court for any damages incurred by a user. If you or your government partner want to modify the content, you need to make sure your content license allows this.
Determine who assumes liability and under what circumstances

Liability — defined as the financial or criminal responsibility an organization assumes for harm or damages caused by its activities — is a frequent concern for partners involved in digital development solutions. Channel partners who publish content or deliver services, such as MNOs, frequently include in their contracts that they are not liable for damages caused by content or service delivery. In fact, most MNO contracts will make you — as the provider of the content or the service — liable if the information given is incorrect or if the service is faulty and results in financial loss or physical harm to the user. In that circumstance, you may need to compensate users for their losses.

Channel partners who publish content or deliver services, such as MNOs, frequently include in their contracts that they are not liable for damages caused by content or service delivery.

If you’re using licensed content or software, you can usually pass the liability to the owner of the content or software. However, most open source software and content licenses absolve their creators of any liability which means that you might be responsible for paying for any losses. On the other hand, if there is a technical fault in the services provided by the MNOs, such as lengthy downtime for interactive voice response or data messages, the MNOs need to assume liability.
In practice | BBC Media Action

The challenges of limiting liability for content and quality of service

One of the biggest challenges BBC Media Action faced when negotiating agreements with six MNOs in India was how to limit liability. Most of the MNOs insisted on using their standard legal templates which exposed us to unlimited liability for our content and the quality of our mHealth education services. This was not something we could agree to, and it took months of legal negotiations to limit this liability.

Content liability was particularly worrying, as the generic clauses provided by the MNOs made us legally responsible for any damages resulting from offense caused to service users. Given that our content deals with sensitive issues such as family planning, it was possible that someone could find the content offensive because of social norms.

Fortunately, our lawyers managed to cap and define our liability. We were able to qualify the clauses relating to offense to state that the content had to comply with the laws of India, and any damage allegedly caused had to be proven in a court of law.

Liability in our MNO contracts for service quality was also a cause for concern because we had to sign up to very tough service level agreements (SLAs). Some of these SLAs insisted on 99.999% up time, fixes to critical faults made within an hour, and financial penalties if we failed to meet the SLAs.

Our aggregator partner was willing to take responsibility legally for its role in meeting these SLAs, but our technical NGO partner — who was responsible for our open source back end system — was not willing to commit, because it had only a small team of engineers based in the United States who worked an eight-hour day. Eventually, our donor agreed to cover their liability and we were able to launch.

Other examples

Watch Kapil Sapra from Kapil Sapra & Associates debunk a myth about liability and compliance when working with government.
Limit and cap liability at a manageable level

At scale and if not clearly limited and capped in your contracts, financial damages resulting from liability can be potentially crippling to your program. The scale of liability will depend on the nature of the service and on how closely associated service providers are with it. For example, if an MNO’s brand colors and logo are on a service, they will be at greater legal risk, however many MNOs’ default position will be that content or mobile technology solution partners accept unlimited liability.

Liability for third-party providers that you contract with for content and software should be as broad as possible, because issues related to these components could have damaging impacts on the entire program. Protect yourself by clearly capping your own liability for things like inaccurate content or faulty service at a well-defined, manageable level in the contract, with no exceptions to the liability cap. Liability insurance also protects your organization if something goes wrong.

Ensure effective indemnification

Defining and agreeing on contractual terms of indemnification — which spell out the conditions under which one party compensates another for losses — can be challenging, and a lawyer’s inputs are especially important here. A key question to ask as you negotiate with new partners is whether you might be held liable for their actions or if a case could be brought against you because of your relationship with them.

Your legal adviser can help develop language that protects you from liability for other parties’ actions or faults. You also need to consider how much control you might have over how your partner responds to legal action. If they take years to resolve an issue, will your digital solution be suspended or lose its reputation in the meantime? Lawyers on both sides will usually try to ensure that indemnification clauses apply to both organizations and that the contract has language that discourages litigation.

Consider the liability of open source vs. proprietary software and content

Using open source software typically requires the user to agree to terms that absolve the creator of that software of any liability. Many digital development programs start by using open source software because the code is available at no cost, but risk for liability expands if the software is modified during the project or if it malfunctions as the program scales. Proprietary software companies, on the other hand, may offer warranties or liability indemnity for their software, which means that they take responsibility for potential damages caused by malfunctioning software. The same conditions may apply to content. Research the pros and cons of open source and proprietary software options to understand what liability providers require you to assume.
A key question to ask as you negotiate with new partners is whether you might be held liable for their actions or if a case could be brought against you because of your relationship with them.
REVIEW AND UPDATE SERVICE LEVEL AGREEMENTS

Define your technical support requirements for scale

Until now, you may not have legally defined technical support for your digital solution. For example, the same software engineers who built your solution may be providing support remotely from another country. But if you are now planning to scale to more users or new geographies or deliver a digital solution at scale on behalf of the government, you need to make sure that you have professional SLAs in place which clearly specify the nature, quantity and quality of support required.

The definition of your support requirements will depend on the type of partner. For example, if you’re partnering with an MNO, you will have to contractually agree to provide the level of support defined in their standard SLAs. Many governments also have tough support requirements that your solution will need to meet if you’re going to deliver services for them at scale.

Ensure your technical partners can meet SLA requirement

Before you contractually agree to comply with MNO or government SLAs at scale, you need to make sure that your technical partners can deliver this level of support. Many open source software development companies don’t have the staff capacity or experience to meet standard MNO SLAs, which can make open source software a risky proposition at scale.

For example, many standard MNO SLAs require nearly 100% service uptime and that you’ll restore the service in one hour if it goes down — at any time of day. Talk to your technical partners about how they are going to meet these requirements.

Watch out for penalty clauses

One reason to be careful about signing up to MNO or government SLAs is that if you fail to meet the terms in them, you are likely to have to pay financial penalties, which will be
In practice | Esoko

Digitizing only reputable sources

In Ghana, we established an external network of subject matter experts (SMEs) that are on our payroll but are not staff. An SLA was signed with each SME or their organizations to ensure that their time was dedicated and their responsibilities were clear. If an SME was to leave an organization or was not able to provide the expert advice that we needed, the SLA ensured that our partner organizations were responsible for replacing the SME. SMEs from the Ghana Meteorological Agency and the Ministry of Food and Agriculture were engaged to approve content for a program to deliver agricultural tips to farmers via SMS and to respond to questions raised by farmers. This agreement reduced our risk of being held liable for any damages caused by incorrect information or misuse of information by farmers, since it came directly from the government.

Other examples

Former leaders at Cell-Life — an NGO that offered technology solutions for health management in low- and middle-income countries — stress the need to think about SLAs. They believe this should be done early in the life of a program and not plan organizational activities around contracts that have not yet been signed. Cell-Life ceased operating in part because an SLA the organization needed to continue the provision and management of a cell-phone-based data collection program for community health workers, took 14 months to clear. By the time the SLA was secured, donor funding for the program had ended. Therefore, the SLA had become useless as Cell-Life no longer had financial resources to take on the project.

Vital Wave worked with an international NGO providing health services to the community and to healthcare workers in Nigeria to scale up the geographical reach of a maternal and neonatal health care call center. When the call center equipment was originally installed in 2010, no SLAs were put into place for long-term maintenance and several pieces of equipment were malfunctioning, had reached end-of-life or were no longer supported by their manufacturers.

Vital Wave purchased new equipment and negotiated an SLA with a technical implementing partner. Since Vital Wave initially contracted the new SLA on behalf of the NGO, the support agreement was made transferrable to the NGO at the end of Vital Wave’s engagement. Ownership of the call center and its SLA has since been transitioned over the government. This highlights both the importance of putting SLAs in place in the beginning of a project and the flexibility provided by making SLAs transferrable. Read more here.

How to

- See an example SLA for members of their external expert network here
- See steps related to drafting an exit provision here
- Read more about risk transfer here
defined in penalty clauses in the agreement. These penalties can raise your operating costs or lower your profits if you’re a social enterprise. If you repeatedly fail to meet your SLAs, your MNO partner could terminate your relationship based on the termination clause in your contract.

On the other hand, you need to ensure that the SLAs for your technical partners are well defined and that adequate penalties have been specified to cover any failure in meeting MNO or government SLAs that may be caused by these partners. Easy termination clauses need to be made part of such third-party contracts.
Before you contractually agree to comply with MNO or government SLAs at scale, you need to make sure that your technical partners can deliver this level of support.
This example of SLAs provided by Box, a cloud-based file sharing platform that supports over 41 million users as of May 2017, shows how a vendor might offer different initial responses depending on the license or contract.

<table>
<thead>
<tr>
<th>Urgent</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition:</strong> An issue that renders the Box Service completely inoperative for all users and no workaround is available.</td>
<td><strong>Definition:</strong> An issue materially impairs substantial features of the Box Service for many users and no reasonable workaround is available.</td>
</tr>
<tr>
<td><strong>Initial response SLA</strong></td>
<td><strong>Initial response SLA</strong></td>
</tr>
<tr>
<td><img src="image" alt="1 hour SLA (24x7x365)*" /></td>
<td><img src="image" alt="2 hour SLA (24x7x365)*" /></td>
</tr>
<tr>
<td><img src="image" alt="2 hour target (9AM - 6PM**)" /></td>
<td><img src="image" alt="4 hour target (9AM - 6PM**)" /></td>
</tr>
<tr>
<td><img src="image" alt="No target (9AM - 6PM**)" /></td>
<td><img src="image" alt="No target (9AM - 6PM**)" /></td>
</tr>
</tbody>
</table>
they have with a client. To support expansion of your digital program, you may need to consider increased levels of service from your vendors.

<table>
<thead>
<tr>
<th>Normal</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition:</strong> An issue that impairs a feature of the Box Service for a few users and a reasonable workaround is available.</td>
<td><strong>Definition:</strong> Minor issue or general question, no impacting people’s ability to use Box.</td>
</tr>
<tr>
<td><strong>Initial response SLA</strong></td>
<td><strong>Initial response SLA</strong></td>
</tr>
<tr>
<td>2 hour SLA (24x7x365)*</td>
<td>No SLA (24x7x365)*</td>
</tr>
<tr>
<td>8 hour target (9AM - 6PM**)</td>
<td>No target (9AM - 6PM**)</td>
</tr>
<tr>
<td>No target (9AM - 6PM**)</td>
<td>No target (9AM - 6PM**)</td>
</tr>
</tbody>
</table>

* English support. Local language, if available in specific region, during Box Weekdays’ business hours  
** Available weekdays, English only
RESOURCE ROLLUP

Who do you need?

Reviewing and updating legal, policy, and regulatory foundations for the next phase of your program means making sure that your employees understand what they need to watch for in contract negotiations and solution updates. But it’s equally important that you have trusted legal advisers who understand your program and have experience with digital programs. Whether you use a law firm or hire in-house counsel, be sure to budget adequately for these activities.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Resource type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master agreement negotiation</td>
<td>Legal Counsel, Digital Director and Project Director</td>
</tr>
<tr>
<td>User consent and data protection policy</td>
<td>Legal Counsel, Project Director, Digital Director</td>
</tr>
<tr>
<td>Intellectual property agreement negotiation</td>
<td>Legal Counsel, Project Director, Digital Director</td>
</tr>
<tr>
<td>Development/revision</td>
<td>Manager, Legal Counsel</td>
</tr>
</tbody>
</table>

Pro tips

• **Don’t cut corners on early legal advice.** The cost associated with getting legal advice early in your expansion or transition may be daunting, but having inadequate contract protection can cost much more later on.

• **Plan ahead for user consent and data protection changes.** Inadequate policies can expose you to legal risk and the possibility of shutdown by governments. Review your policies in these areas when you upgrade your solution design and talk to government partners early. It may be safest to adopt best practices early on, regardless of the current state of legislation in your geographies.

• **Pay attention to content IP and liability too.** Some digital development leaders report that they focused on software-related IP and liability as they grew and didn’t devote enough attention to content IP and liability, which can take a long time to negotiate. If you’ll be developing or acquiring a lot of new content in the next phase, talk to your lawyers early about what this will entail.
<table>
<thead>
<tr>
<th>Key step</th>
<th>Referenced resources</th>
</tr>
</thead>
</table>
| 1. ASSESS THE IMPACT OF EVOLVING LAWS, POLICIES AND REGULATIONS ON COMPLIANCE | - Case Study: mHealth Compendium Volume Four (Anaya: Shaping Life-Saving Reproductive, Maternal, Newborn and Child Health Practices and Behaviors in India)  
- Case Study: MomConnect: Launching a National Digital Health Program in South Africa  
- Paper: Data Localization: A Challenge to Global Commerce and the Free Flow of Information (Global Spread of Data Localization)  
- Case Study: Kilkari: A maternal and child health service in India – Lessons learned and best practices for deployment at scale  
- Example: Information Regulator (South Africa) Documents  
- Paper: Mobile Privacy Principles  
- Example: Informed Consent Resource Library  
- Paper: International Compilation of Human Research Standards |
| 2. ENSURE A FLEXIBLE CONTRACTING APPROACH TO ACCOMMODATE CHANGE | - Paper: Change Control Process  
- Example: Sample Master Services Contract for IT Services |
| 3. CLARIFY OWNERSHIP OF INTELLECTUAL PROPERTY | - Case Study: mHealth Compendium Volume Four (Anaya: Shaping Life-Saving Reproductive, Maternal, Newborn and Child Health Practices and Behaviors in India)  
- Tool: WIPOLex  
- Example: Work for Hire Agreement  
- Example: Intellectual Property Assignment Agreement Template  
- Example: Intellectual Property Sale Agreement Template |
<table>
<thead>
<tr>
<th>Key step</th>
<th>Referenced resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. REVIEW SOFTWARE, HARDWARE AND CONTENT</td>
<td>• Example: Content License Agreement</td>
</tr>
<tr>
<td>LICENSING TERMS</td>
<td>• FAQ: Creative Commons Licenses for Global Health Content</td>
</tr>
<tr>
<td></td>
<td>• Article: 3 Tensions with Software Sustainability in ICT4D</td>
</tr>
<tr>
<td>5. CLARIFY, LIMIT AND MANAGE LIABILITY</td>
<td>• Tool: Contract Self-assessment Checklist</td>
</tr>
<tr>
<td></td>
<td>• Example: Sample Indemnity/Insurance Clause</td>
</tr>
<tr>
<td></td>
<td>• Article: Why Your Contract Should Contain an Indemnification Clause</td>
</tr>
<tr>
<td></td>
<td>• Paper: Legal Liability Issues of Mobile Application Relationships in Europe</td>
</tr>
<tr>
<td>6. REVIEW AND UPDATE SERVICE LEVEL AGREEMENT</td>
<td>• Case Study: Expansion and Implementation Support for a Health-Focused Call Center in Nigeria</td>
</tr>
<tr>
<td></td>
<td>• Example: Esoko Expert Network Service Level Agreement</td>
</tr>
<tr>
<td></td>
<td>• Article: Seven Key Questions for Drafting Effective Exit Provisions</td>
</tr>
<tr>
<td></td>
<td>• Article: Risk Transfer: A Strategy to Help Protect Your Business</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Addenda</td>
<td>An addition to a completed written document. Most commonly, this is a proposed change or explanation (such as a list of goods to be included) in a contract or some point that has been subject of negotiation after the contract was originally proposed by one party. Although often they are not, addenda should be signed separately and attached to the original agreement so that there will be no confusion as to what is included or intended. Unsigned addenda could be included fraudulently or confused with rough drafts or unaccepted proposals.</td>
</tr>
<tr>
<td>Aggregator</td>
<td>An organization that acts as a middleman between application and content providers, and mobile carriers. Provides message traffic throughput to multiple wireless operators or other aggregators; provides mobile initiative campaign oversight, and administration, as well as billing services.</td>
</tr>
<tr>
<td>Annexes</td>
<td>A document appended to another document to make it clearer or to give further details.</td>
</tr>
<tr>
<td>Assignment and assumption</td>
<td>An assignment and assumption agreement transfers one party’s rights and obligations under a contract to another party. The party transferring their rights and duties is the assignor; the party receiving them is the assignee. Sometimes, an assignor is not completely relieved of liability even after they assign a contract. Parties must look to a contract’s specific language to determine applicable restrictions, terms and conditions for assignments and assumptions.</td>
</tr>
<tr>
<td>Creative Commons (CC)</td>
<td>One of several public copyright licenses that enable the free distribution of an otherwise copyrighted work. A CC license is used when an author wants to give people the right to share, use and build upon a work that they have created. CC provides a creator flexibility and protects the people who use or redistribute another’s work from concerns of copyright infringement as long as they abide by the conditions that are specified in the license by which the creator distributes the work.</td>
</tr>
<tr>
<td>End-of-life</td>
<td>A term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life (from the vendor’s point of view), and a vendor stops marketing, selling, or rework sustaining it.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Indemnity, indemnification</td>
<td>To guarantee against any loss which another might suffer. Example: Two parties settle a dispute over a contract, and one of them may agree to pay any claims which may arise from the contract, holding the other harmless.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Intellectual property (IP)</td>
<td>Any of various products of the intellect that have commercial value, including copyrighted property such as literary or artistic works, and ideational property, such as patents, business methods and industrial processes.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Made for hire</td>
<td>Work subject to copyright that is created by an employee as part of his job, or some limited types of works for which all parties agree in writing to the designation. Also known as work for hire and work made for hire.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Service level agreements (SLAs)</td>
<td>A contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based specifically defining what the customer will receive. SLAs do not define how the service is provided or delivered. The metrics that define levels of service should aim to guarantee a description of the service being provided, reliability, responsiveness, procedure for reporting problems, monitoring and reporting service level, consequences for not meeting service obligations, and escape clauses or constraints.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Statement of work (SOW)</td>
<td>A document routinely employed in the field of project management. It defines project-specific activities, deliverables and timelines for a vendor providing services to the client. The SOW typically also includes detailed requirements, pricing, and standard regulatory and governance terms and conditions.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Termination clauses</td>
<td>Contract provision allowing it to be terminated under certain circumstances. Also known as terminate provision.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Work for hire</td>
<td>See Made for hire.</td>
</tr>
</tbody>
</table>